SCCM Proposed Time line

1. Wednesday 21st
   a. Change Default Update Deployment GPO to point to new SCCM server.
   b. Start new client push out.
   c. Change/remove any outdated GPO’s to old system.
2. ASAP
   a. Get list of test machines from area techs for Updates.
3. Feb 5th
   a. SCCM Go Live
   b. This is the date area techs can go to the new SCCM to start making packages and deployments.

New server is SCCM.ad.uvu.edu
Console installer is at: `\sccm\ConsoleSetup`

The security department has asked that we look at the way Admin rights are being applied to the Desktops across campus. The affected GPO’s are listed below:

**GPO: “Default rename local Administrator”**

This GPO renames the local “Administrator” account to “UVUAdmin” for Windows 7, 8, and 8.1 only. It is applied at the DEPT container. It sets the following for that user: User cannot change password = False; Password never expires = True; Account is disabled = False; Account expires = Never. It does not set a password.

**GPO: “Default Allow Only Employee Logon”**

This GPO allows “BUILTIN\Administrators” and “AD/1” users to log on locally and is applied to the following containers: Adjunct, Administration, CCRR, CHSS, Concurrent Enrollment, Continuing Education, CTE, Distance Education, Science, Student Life, and Turing Point.

**GPO: “Default Employee Local Administrators”**

This GPO adds the “AD/1” group to the local Administrators Group. It is applied to 33 different containers, none at the “DEPT” level.

Proposed changes to be made March 1st:

1. **GPO: “Default rename local Administrator”**
   a. Change the “Default rename local Administrator” GPO so “User cannot change password = True” and “Account is disabled = True”.
2. **GPO: “Default Allow Only Employee Logon”**
   a. Remove “AD/1” from this GPO. If an area technician wants to allow an IDM group local access to a desktop a new GPO should be created at their level.
3. **GPO: “Default Employee Local Administrators”**
   a. Delete this GPO completely.